



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/634,841	08/08/2000	Takuya Wada	SON-1887	4733

7590 05/14/2004

RADER, FISHMAN & GRAUER, P.L.L.C.  
Suite 501  
1233 20th Street, NW  
Washington, DC 20036

EXAMINER

DINH, MINH

ART UNIT PAPER NUMBER

2132

DATE MAILED: 05/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/634,841

Applicant(s)

WADA ET AL.

Examiner

Minh Dinh

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 August 2000 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_.

**DETAILED ACTION**

1. Claims 10-20 have been examined.

***Drawings***

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: reference numeral "100" (figure 1). A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference numerals mentioned in the description: "6" (see page 15, third line from bottom) and "56" (page 19, line 11). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

***Specification***

4. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless – (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1 and 11 are rejected under 35 U.S.C. 102(e) as being anticipated by Borza et al. (6,215,874). Regarding claim 1 which is representative of claim 11, Borza discloses an apparatus comprising:

pick-up means (fig. 1, element 1);

digital image conversion means for converting into a digital image a pick-up signal output from said pick-up means (col. 6, lines 45-51);

storage means for storing digital values correlated to a plurality of pixels in the digital image (col. 6, lines 45-51); and

random number generating means for extracting a digital data from pixel values of a plurality of pixels in the digital image of said pick-up signal output when no subject is present from said pick-up means stored in said storage means, and generating a random number from the digital data correlated to the plurality of pixels (fig. 4a; col. 4, lines 52-56; col. 6, lines 21-26).

Art Unit: 2132

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 2-3 and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Borza as applied to claims 1 and 11 above, and further in view of Nielsen (5,774,549).

a. Regarding claims 2 and 12, Borza does not disclose that the pixel values are express by 2 or more bits, and the random number generating means extracts as said digital data binary data of the least significant bits of a bit string expressing the pixel values and generates a random number from the binary data. Nielsen discloses an image comprising of pixels having pixel values express by 2 or more bits, and means for extracting the least significant bits to generate a random number generator seed, which meets the limitation of a random number (col. 3, lines 9-15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Borza such that the pixel values are express by 2 or more bits, and the random number generating means extracts as said digital data binary data of the least significant bits of a bit string expressing the pixel values and generates a random number from the binary data, as taught by Nielsen, so that it could operate without regard to the depth of the color component representation (col. 3, lines 15-17).

b. Regarding claims 3 and 13, Borza does not disclose that the digital image is a binary image in which the pixel values are express as 1-bit binary data, and the random number generating means extracts the binary data as said digital data and generates a random number from the binary data. Nielsen discloses a monochrome image in which the pixel values are express as 1-bit binary data, the image meets the limitation of a binary image, and the random number generating means extracts the binary data as said digital data and generates a random number from the binary data (col. 3, lines 18-22). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Borza such that the digital image is a binary image in which the pixel values are express as 1-bit binary data, and the random number generating means extracts the binary data as said digital data and generates a random number from the binary data, as taught by Nielsen, so that it could operate without regard to the depth of the color component representation (col. 3, lines 15-17).

9. Claims 4-5 and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Borza as applied to claims 1 and 11 above, and further in view of Wakasu (6,259,801). Regarding claims 4 and 14, Borza does not disclose that data is extracted from a predetermined area or at an arbitrary position within the digital image. Wakasu discloses means for extracting data from a predetermined area or at an arbitrary position within a digital image (fig. 2). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Borza such that data is extracted from a predetermined area or at an arbitrary position within the

digital image, as taught by Wakasu, so that different kind of embedded data could be detected properly (col. 4, lines 51-56).

10. Claims 6, 9-10, 16 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Borza as applied to claims 1 and 11 above, and further in view of Tomko et al. (5,541,994).

a. Regarding claims 6 and 16, Borza does not disclose that the apparatus is provided in an encryption block for generating an encryption key according to data obtained from the random number. Tomko discloses an apparatus comprising a random number generator and an encryption key generator that generate keys according to data obtained from the random number, the apparatus meets the limitation of an encryption block (fig. 2, elements 84 and 88). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Borza such that an encryption key generator is provided to generate encryption keys according to data obtained from the random number generator, as taught by Tomko, so that encryption keys could be generated and transmitted to the other entity of a secure communication (col. 6, lines 12-17).

b. Regarding claims 9-10 and 19-20, Borza further discloses a subject picked up by the pick-up means being a fingerprint (col. 4, lines 28-30). However, Borza does not disclose that the apparatus is provided in an individual identification apparatus according to a digital image correlated to a fingerprint picked up by the pick-up means, and the individual identification apparatus performing an encryption of a plain text using

the encryption key when a desired individual is identified. Tomko discloses a random number generator provided in an individual identification apparatus according to a digital image correlated to a fingerprint picked up by the pick-up means, and the individual identification apparatus performing decryption of an encrypted message using a private key when a desired individual is identified (fig. 2). Tomko does not disclose using the private key to encrypt a plain text. However, Examiner takes Official Notice that using a private key to encrypt a message is well known for the purpose of generating a secure digital signature, which is applicable to the invention. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the apparatus of Borza in an individual identification apparatus according to a digital image correlated to a fingerprint picked up by the pick-up means, and the individual identification apparatus performing an encryption of a plain text using the encryption key when a desired individual is identified, as taught by Tomko, since Examiner takes Official Notice that the use of a private key to encrypt a message is well known. The motivation for doing so would have been to provide a public key cryptography system which generates a secure and readily accessible private key (col. 1, lines 64-67).

11. Claims 7 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Borza in view of Tomko as applied to claims 6 and 16 above, and further in view of Schneier ("Applied Cryptography"). Borza and Tomko do not disclose using the RSA encryption method for generating the encryption key using two random prime numbers. Schneier discloses using the RSA encryption method for generating the encryption key



Art Unit: 2132

using two random prime numbers (section 19.3 RSA, page 467). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Borza to use the RSA encryption method for generating the encryption key, as taught by Schneier, because it is by far the easiest to understand and implement (section 19.3 RSA, page 466).

12. Claims 8 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Borza in view of Tomko as applied to claims 6 and 16 above, and further in view of Epstein (US 2002/0124176 A1). Borza and Tomko do not disclose that the apparatus comprises custody means for keeping the encryption key in custody. Epstein discloses custody means for keeping an encryption key in custody (par. 0018). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Borza to include use custody means for keeping the encryption key in custody, as taught by Epstein, for gaining access to a security system (Abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

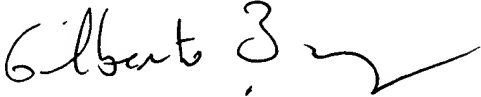
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh  
Examiner  
Art Unit 2132

MD  
05/10/2004

  
GILBERTO BARRÓN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100